# INTERNET RZECZY WYZWANIEM DLA INFRASTRUKTURY KRYTYCZNEJ? DIGITALIZACJA JEST NIEUCHRONNA

„Decydując się na urządzenia pracujące w sieci, musimy mieć świadomość, że cyberbezpieczeństwo jest ich nierozerwalną częścią" – podkreślił w rozmowie dla CyberDefence24.pl Jacek Łukaszewski, prezes Klastra Schneider Electric na Polskę, Czechy, Słowację, Ukrainę. Odniósł się również do ryzyka związanego z wykorzystaniem urządzeń zaliczanych do Internetu Rzeczy w branży energetycznej oraz znaczenia innowacji w tym segmencie gospodarki. „Infrastruktura krytyczna coraz szybciej się digitalizuje" – wskazał przedstawiciel sektora prywatnego.

**Ilość usług, jakie świadczy Schneider Electric oraz liczba produktów dostarczanych przez firmę sprawia, że kwestia funkcjonowania w cyberprzestrzeni jest zjawiskiem nieuniknionym. Wynika to między innymi z wykorzystania urządzeń należących do kategorii Internetu Rzeczy (ang. Internet of Things, IoT). My, jako Polacy, nie do końca jeszcze rozumiemy czym tak naprawdę jest IoT i jak w jaki sposób działa. A jak wygląda świadomość na temat tej technologii w Schneider Electric? Czy z perspektywy Pana firmy IoT ma potencjał?**

Dwa obszary, którymi zajmuje się Schneider Electric to zarządzanie energią i automatyką. Internet Rzeczy to nic innego jak umożliwienie komunikacji całemu szeregowi przedmiotów, maszyn i itd. Z perspektywy konsumenta mówimy na przykład o zegarkach czy smartfonach, które de facto mają możliwość mierzenia tego, co się z nimi dzieje, czyli zmiennych środowiskowych takich jak wilgotność, temperatura, ciśnienie. Tego typu przedmioty informują użytkownika o określonym stanie i przekazują je dalej. Mówimy więc o urządzeniach, które dokonują pomiaru parametrów – środowiskowych lub procesowych – i kierują pozyskane dane do kolejnych urządzeń, serwerów, odpowiedzialnych za ich przetwarzanie. Następnie na podstawie otrzymanych informacji wykonują jakiś proces lub archiwują określone pomiary.

Wspomniany wyżej proces występuje w automatyce przemysłowej od lat 60., kiedy ta dziedzina powstała. Różnica polega na tym, że w przeszłości było to bardzo kosztowne, ponieważ każde urządzenie pomiarowe było drogie. To samo dotyczyło komunikacji, która nie była tania. Obecnie komunikacja to Internet, a więc dzięki niemu mamy ogólny standard w tym obszarze. Dodatkowo urządzenia pomiarowe zdecydowanie staniały, co ma niebagatelny wpływ na cały proces.

Proszę zauważyć, że w dzisiejszych czasach każdy nosi przy sobie telefon, który dokonuje pomiaru kilkunastu wartości fizycznych. Posiada kamerę, czyli jest w stanie rejestrować obraz; czujnik GPS, a więc potrafi określić położenie geograficzne; ma akcelerometr i cały szereg innych funkcji. To wszystko zalicza się do Internetu Rzeczy, ponieważ po pierwsze technologia czujników staniała, a po drugie komunikacja stała się powszechna.

W Schneider Electric trend czynienia produktów inteligentnymi, czyli wyposażania ich w możliwości analizy informacji oraz zdolności komunikacyjne, występuje praktycznie od zawsze. Od kilkunastu lat prowadzimy działalność w dwóch podstawowych obszarach: zarządzania energią, w tym dystrybucji energii w sferze automatyki. Wobec tego, jeśli spojrzymy na nasze produkty, to każda następna generacja jest bardziej „inteligenta" i ma coraz większe możliwości pomiarowe, przetwarzania danych oraz komunikacyjne.

W latach 80. jako jedna z pierwszych firm wyposażyliśmy nasze sterowniki przemysłowe w standard Ethernet, kiedy był uznawany jako absolutnie niezbędny do sterowania przemysłowego. Jeżeli spojrzymy na aparaturę modułową, czyli wszystkie elementy, które każdy z nas ma w szafkach elektrycznych, to aktualna seria Schneider Electric posiada cały szereg inteligentnych urządzeń. Nazywają się „Smartlink" i pozwalają na skuteczną komunikację. W ten sposób aparatura może informować o stanie instalacji elektrycznej, może też mierzyć energię i podejmować inne działania.

Dobrym przykładem wzrostu „inteligencji" urządzeń jest licznik elektryczny. Każdy z nas ma takie urządzenie w domu, ponieważ konsumujemy energię. Jeżeli spojrzymy na tego typu urządzenie sprzed 20 lat, to było ono elektro-mechaniczne. Mierzyło energię czynną, czyli de facto jedynie jedną fizyczną cechę prądu elektrycznego zużytą w określonym czasie. Z kolei gdy spojrzymy na te nowoczesne, inteligentne liczniki, to oczywiście podstawowa funkcja (mierzenie energii czynnej – przyp. red.) jest zapewniona. Jednak to urządzenia, które – po pierwsze – są elektroniczne, mierzą kilkanaście lub nawet kilkadziesiąt wartości fizycznych dotyczących prądu elektrycznego. Poza energią czynną dokonują pomiaru energii biernej, napięcia, natężenia, częstotliwość i szeregu innych wartości. Po drugie, wiele z tych urządzeń komunikuje się nie za pośrednictwem wyświetlacza, tylko po protokole, niezależnie czy jest to magistrala licznikowa czy radiowa.

Oczywiście wyposażenie tych urządzeń w możliwości analizy danych i zdolności komunikacji otwiera cały szereg nowych możliwości w zakresie funkcjonalności. Należy podkreślić, że ta podstawowa funkcjonalność, to znaczy pomiar zużytej energii elektrycznej do tego, żeby wystawić rachunek, jest oczywiście spełniona. Do całości następnie dochodzi szereg innych rzeczy.

Obecnie każda nowa generacja produktów Schneider Electric zaczyna być smart, dlatego że możliwości technologiczne pozwalają wyposażać je w „inteligentne" rozwiązania, co z kolei pozwala zwiększyć funkcjonalność. Mówiąc konkretnie, urządzenia zaczynają mieć więcej funkcji, na których użytkownik korzysta w różny sposób, na przykład w zakresie niezawodności, aktywności zużycia, komfortu czy bezpieczeństwa.

**Biorąc po uwagę, że mamy pięciu dużych, głównych sprzedawców energii – jaki jest procent wykorzystania liczników typu „smart"? Czy posiada Pan wiedzę na ten temat?**

Niestety trudno jest uzyskać tego typu dane. My, jako Schneider Electric, liczników dla operatorów sieci energetycznych nie sprzedajemy. Za to jesteśmy jednym z liderów sprzedaży systemów analizy zużycia i jakości energii. W związku z tym bardzo często działamy po stronie użytkownika. Przykładowo, wyobraźmy sobie sieć sklepów – 100 identycznych sklepów w Polsce, każdy z nich ma inne zużycie energii i właściciel zaczyna się zastanawiać, w jaki sposób zoptymalizować wydatki za energię, bo na przykład prąd drożeje. W takiej sytuacji system monitoringu pozwala między innymi zdiagnozować konsumowanie energii, można powiedzieć, że umożliwia „śledzenie" zużycia.

Bardziej skomplikowanym problemem jest zakład przemysłowy czy serwerownia, gdzie jakość energii ma kluczowe znaczenie ze względu na fakt, że wpływa na funkcjonowanie podstawowych urządzeń. Wówczas posiadanie systemu monitoringu energetycznego umożliwia nie tylko efektywnie tą energią zarządzać, ale również pozwala udowodnić dostawcy, że jest ona nieodpowiedniej jakości. W ten sposób właściciel danej placówki może żądać rekompensaty lub domagać się innych roszczeń.

System monitoringu generalnie pozwala na zdiagnozowanie różnych problemów z mocą bierną lub innych niepożądanych efektów. To z kolei sprawia, że znając problem, można wdrożyć odpowiednie rozwiązania zaradcze.


Prezes zarządu Schneider Electric Polska Jacek Łukaszewski/ Fot. Schneider Electric

**Jeśli poruszamy się w tematyce systemów, to jak wygląda kwestia ich funkcjonowania z punktu widzenia cyberbezpieczeństwa? Pojęcie „cyber" jest hasłem, które obecnie zyskało dużą popularność. W związku z tym jak wygląda ten obszar ze strony Schneider Electric? Firma nie padła ofiarą poważnego incydentu, lecz czy mógłby Pan odnieść się do problematyki ryzyka. Jaka jest podatność urządzeń?**

Generalnie technologie czy wyposażenie urządzeń w możliwości przetwarzania danych, czyli wdrażanie innowacji oraz otwieranie się na komunikację, niesie ze sobą ryzyko. Każdy z użytkowników musi mieć tego świadomość. Niepodważalny jest fakt, że częścią cyfryzacji jest oczywiście cyberbezpieczeństwo.

W tym miejscu pragnę podkreślić, że bardzo wiele naszych urządzeń pracuje w obszarze infrastruktury krytycznej. Odcięcie energii elektrycznej na skutek cyberataku jest czymś realnym. Były tego typu przypadki w przyszłości, między innymi największy z ataków DDoS został przeprowadzony przez boty, które były zainstalowane na kamerach i routerach, czyli na urządzeniach sieciowych. Na Ukrainie doszło do wyłączenia sieci energetycznej poprzez ransomware. Tak więc widzimy, że tego typu rzeczy w cyfrowym świecie się zdarzają.

Schneider Electric bardzo poważnie traktuje cyberbezpieczeństwo. Potwierdzeniem tego może być fakt, że na przykład jako jedna z niewielu firm w sterownikach przesyłowych gwarantujemy szyfrowanie transmisji, zaimplementowane już na poziomie sterownika. Mówiąc prościej, nasze

produkty posiadają wbudowaną technologię *cyber security*. Co więcej, staramy się te urządzenia certyfikować w odpowiednich – czy to branżowych czy to państwowych – instytucjach. W ten sposób widać, że Schneider Electric z jednej strony nadąża za tym, co się dzieje w „świecie technologii", z drugiej strony certyfikując swoje urządzenia, regularnie je bada i sprawdza jakość.

**W Polsce podmiotem certyfikującym jest Instytut Łączności?**

W Polsce akurat tego typu urządzeń nie produkujemy, wobec czego certyfikacja nie występuje. Ale jeśli chodzi na przykład o sterowniki przemysłowe, to w ostatnim czasie jeden z dużych międzynarodowych klientów, który jest graczem na rynku IT i rozwija działalność w Polsce, nasze produkty w pełni zaaprobował, wyłącznie z uwagi na fakt zagwarantowania technologii szyfrowania w ramach urządzenia. To nie jest jeszcze standard. Obecnie jesteśmy jedną z niewielu firm, która to posiada.

**Najlepszym przykładem odnoszącym się do cyberbezpieczeństwa w branży była sytuacja z udziałem firmy „Energa". Przetestowała ona 2000 liczników radiowych, które można było bardzo łatwo zhakować. Wynikało to z faktu, że ustawiono proste dane dostępu – login: admin, hasło: admin. W związku z tym, jeśli w urządzeniach Schneider Electric występuje szyfrowanie na poziomie urządzenia końcowego, to tego typu problem bądź ryzyko jest zdecydowanie mniejsze.**

Problem zawsze występuje, dlatego że technologia nieustannie idzie do przodu. Decydując się na urządzenia pracujące w sieci, musimy mieć świadomość, że cyberbezpieczeństwo jest ich nierozerwalną częścią. W związku z tym jest istnieje szereg działań, które musimy podejmować po to, żeby chronić naszą infrastrukturę. Co więcej, postęp technologiczny wymaga inwestycji, aby nadążać za aktualnie pojawiającymi się nowinkami.

**Schneider Electric posiada w swoich urządzeniach rozwiązania z zakresu cyberbezpieczeństwa, które są dodatkowo certyfikowane. Jakie istnieją jeszcze inne sposoby zabezpieczenia produktów w Państwa firmie?**

Tak jak już wspomniałem wcześniej, wiele naszych urządzeń pracuje w ramach infrastruktury krytycznej. Co więcej, ta infrastruktura krytyczna coraz szybciej się digitalizuje. Dostrzegamy, że wielu klientów w tym obszarze nie ma ani doświadczenia ani wiedzy. Z drugiej strony, spora ilość podmiotów, które się specjalizują w bezpieczeństwie cyfrowym była głównie nastawiona na branże IT.

Obecnie „styk" technologii operacyjnej (OT) i IT jest czymś, co postrzegamy jako część naszych kompetencji. W związku z tym posiadamy globalny dział usługowy cyberbezpieczeństwa, gdzie doradzamy klientom z branży przemysłowej czy z sektora dystrybucji mediów, spółek energetycznych i innych, w jaki sposób wdrażać rozwiązania *cyber security*, kiedy coraz więcej urządzeń zaczyna być inteligentnych. Oczywiście ich wykorzystanie niesie ze sobą wiele zalet, ale równocześnie wymaga odpowiednich działań w zakresie bezpieczeństwa.

**Uważa Pan, że trzeba wprowadzić normy, które miałyby na celu – na poziomie Polski czy Unii Europejskiej – uregulowanie kwestii minimalnych standardów w tym obszarze?**

Generalnie uważam, że certyfikacja to przyszłość, dlatego że trudno wymagać, żeby każdy klient budował u siebie specjalistyczny zespół ekspertów, dokonywał analizy technologii i wdrażał własne rozwiązania lub innych firm. W związku z tym powinny być ustalone standardy, czy to sektorowe czy branżowe, ponieważ różne rozwiązania pasują do różnych obszarów. Wówczas firmy takie jak Schneider Electric, dostawcy sprzętu, de facto powinny przedstawiać zgodność z certyfikatami.

Oczywiście obecnie istnieją pewne normy międzynarodowe jak na przykład ISO 27001. Jednak

uważam, że zarówno od strony UE jak i Polski powinno istnieć bardzo systemowe podejście. Całość wymaga dużego nakładu pracy, ponieważ jest to przysłowiowe „gonienie uciekającego króliczka”.

**„Albo go dogonisz albo nigdy nie wyprzedzisz…”**

Zgadza się. Jestem zdania, że z czasem będzie dużo lepiej. Odnosząc się do jednostki, która ustala certyfikaty, możemy sobie wyobrazić, że na poziomie międzynarodowym, czyli na przykład UE, jest duże grono specjalistów, którzy się tym zajmują. Obserwują jak wyglądają technologie, analizują, wyciągają wnioski, a potem określają poziom certyfikacji i wtedy powstaje konkretna wytyczna dla biznesu. Wówczas środowisko biznesu nie musi dokonywać analiz tych technologii samodzielnie. To zdecydowanie uporządkuje rynek, ale też z jednej strony pomoże firmom wybrać odpowiednie technologie, a z drugiej zwiększony system certyfikacji podniesie świadomość.

W tym miejscu chciałbym jeszcze raz podkreślić, że częścią cyberbezpieczeństwa jest kwestia świadomości zarówno kupujących jak i użytkujących konkretne urządzenia czy systemy. *Cyber security* to nie jest tylko sprawa możliwości sprzętu, ale też określonego zachowania użytkowników. Jak wiemy, większość włamań następuje nie dlatego, że „sprzęt się nie broni”, tylko dlatego, że ludzie wykonują określone działania w sposób nieprawidłowy, umożliwiając hakerom działanie.

Technologie cyfrowe niosą cały szereg zalet i nie sądzę, że możemy żyć w XXI wieku, nie korzystając z nich. Również w branży przemysłowej i zarządzania energią nie ma odwrotu od innowacji. Jeżeli spojrzymy na to, co się obecnie dzieje w energetyce, to technologia cyfrowa jest jedyną drogą naprzód, która pozwala zarządzać siecią wyposażoną na przykład w odnawialne źródła energii.

**Dziękuję za rozmowę.**

Dziękuję.

W oświadczeniu przesłanym do redakcji firma Energa Operator napisała, że nie stosuje liczników radiowych, zaś transmisja z licznikami GSM odbywa się w obrębie prywatnej sieci APN. Zgodnie z polityką bezpieczeństwa wykorzystywane są standardy, które uniemożliwiają dostęp osobom trzecim do przetwarzanych danych. Standardy te dotyczą również używania odpowiedniej liczby i rodzaju znaków w hasłach oraz czasu ich ważności.